Hacking en redes conmutadas

Angel Alonso Párrizas
parrizas@wanadoo.es
http://angelillo.no-ip.org

Introducción

El uso de conmutadores es seguro frente a sniffers

No en todos los casos todos los conmutadores son la panacea

Veremos como se puede capturar tráfico en una red ethernet conmutada.

¿Qué soluciones hay?

Otros ataques. Ejemplos de sniffers

¿Cómo podemos detectar estos ataques?

Bibliografía y referencia web.

Conclusiones

Bibliografía

http://www.seg.inf.uc3m.es/spi/sniffers/EnvenenamientoARP.html Arp Poison

http://bulmalug.net/body.phtml?nIdNoticia=1193 Hacking en redes conmutadas

http://www.governmentsecurity.org/articles/TheIngredientstoARPPoison.php The ingredents to ARP-Poison

http://packetstormsecurity.nl/papers/general/Altering_ARP_Tables_v_1.00.htm Altering ARP tables

http://www.cyruxnet.com.ar/ettercap.htm usando Ettercap

http://www.cyruxnet.com.ar/cuaderno3.htm Man in the middle.

http://www.monkey.org/~dugsong/dsniff/ Dniff. Alternativa a Ettercap.

http://archive.infoworld.com/articles/op/xml/00/05/29/000529opswatch.xml Switched networks lose their security advantage due to packet-capture

http://slashdot.org/articles/00/12/18/0759236.shtml Attack against SSH1 and SSL

http://secinf.net/info/misc/sniffingfaq.html (punto 3.8) How can I sniff a switched network?

http://cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_5_4/config/sec_port.pdf Conmutadores cisco y configuración óptima.

http://www.ovislinkcorp.es/productos/producto.php?categoria=switch&id=11 Características conmutador Ovislink

http://www.ovislinkcorp.es/productos/pdf/fsh2400.zip Manual conmutador ovislink.

http://usuarios.lycos.es/elvenbyte/index.php?pagina=stp Ataques de spanning tree.

http://packetstorm.securify.com/NT/snarp.zip Sniffer mediante ARP-poison para windows NT

Redes de computadores. Andrew S. Tanenbaum. Tercera edición. ISBN: 968-880-958- (pag 423-433)

Network Intrusion Detection. Stephen Northcutt & Judy Nobak. 3ª edición. ISBN:0-7357-1265-4

Nuestro escenario 1

Red en casa de cultura dependiente del consistorio municipal.

- PC dirección casa de cultura.
- PC oficina de turismo.
- 8 PCs ubicados en la bilioteca. Libre acceso a Internet. No instalar software.
- 2 PC's consulta biblioteca, videoteca, Cdteca, DVD's
- 1 PC Bibliotecario para altas/bajas.
- 2 puestos libres para portátiles.

Conmutador LAN ovislink Ether-FSH24RS con 24 puertos 10/100.
(http://www.ovislinkcorp.es/productos/producto.php?categoría=switch&id=11)

Router ADSL 3com 812 con línea de 2Mbits/s.

Nuestro escenario 2

- Servidor Linux (Debian 3.0)
  - DNS, Bind9. Se tiene un dominio registrado.
  - DHCP. Parar asignar las ip's de todas las máquinas de la red local.
  - Exim. Gestión del correo con el nombre de dominio adquirido.
  - Apache. Ver: 1.3.27. Páginas web del ayuntamiento y biblioteca.
  - MySQL. Base de datos de libros y usuarios (120Megabytes). Algunas webs interactúan mediante PHP.
  - Telnet: Administración del servidor.
  - Núcleo 2.4.18-bf4 (por defecto la que trae la distribución).
  - Iptables. Hacemos NAT a la red local y filtramos tráfico como P2P.

Nuestro escenario 3

La red siempre ha funcionado bien, exceptuando las veces que se cae el ADSL.

...hasta que un día y en momentos concretos el acceso a la base de datos era imposible..

- Comprobamos autonegociación y forzamos manual

```
root@servidor:~$ mii-tool
 eth1: 100 Mbit, Full duplex, link ok
```

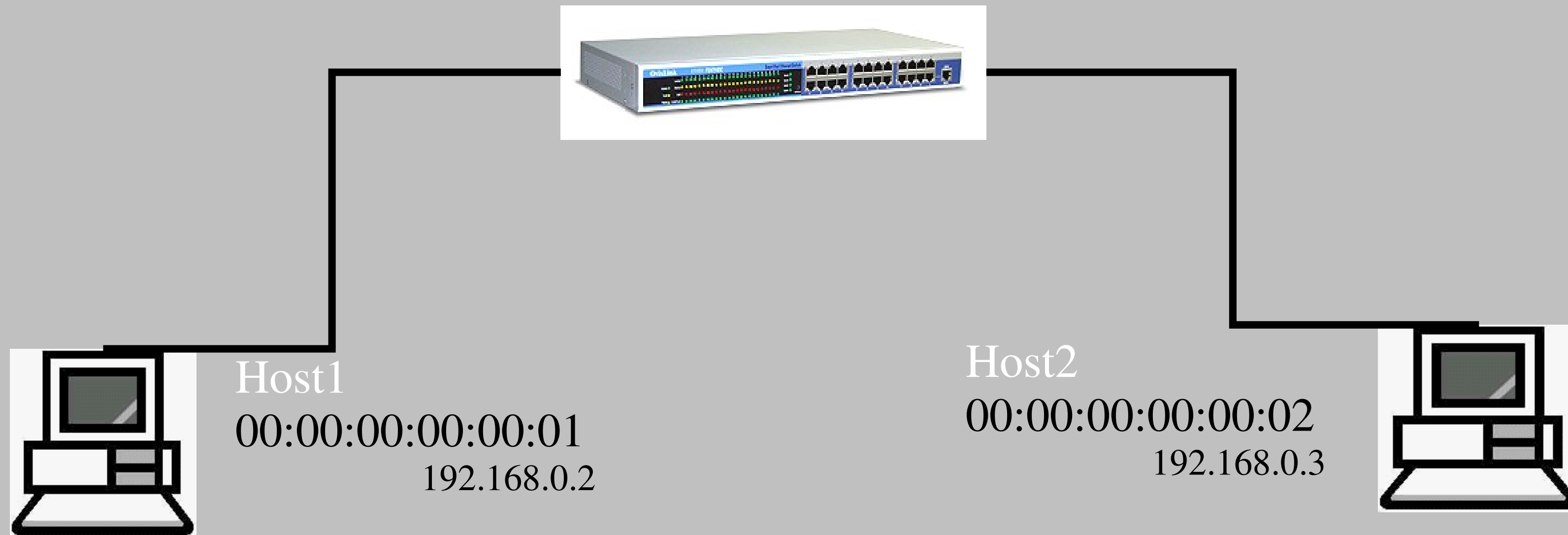
- El problema no era éste, porque sólo ocurría en momentos muy concretos. Cuando los usuarios de portátiles se conectaban.
  - ¿Problema de DHCP y conflicto de IP's?

Un usuario en concreto usaba una aplicación desconocida para nosotros. Ettercap

¿Que es ettercap?

- Sniffer que funciona bajo un ataque llamado ARP-poison (envenenamiento ARP)
- El ataque arpovecha el protocolo ARP (Address Resolution Protocol)
- ARP nos devuelve la MAC de una tarjeta que tiene una dirección IP.
  - Se envía un paquete ARP a la dirección broadcast FF:FF:FF:FF:FF:FF
  - Pero cada máquina guarda en su caché el par MAC/IP durante un tiempo.
  - Aunque no efectuemos un ARP-Request en nuestra caché se guardan los datos igual.
  - Lo que hacemos es falsear ARP con la MAC del atacante de modo que el tráfico pasa por el ordenador espía.

Funcionamiento ARP



H1 envía un paquete ARP-Request a la dirección broadcast preguntando cual es la MAC de la tarjeta que tiene como ip 192.168.0.3

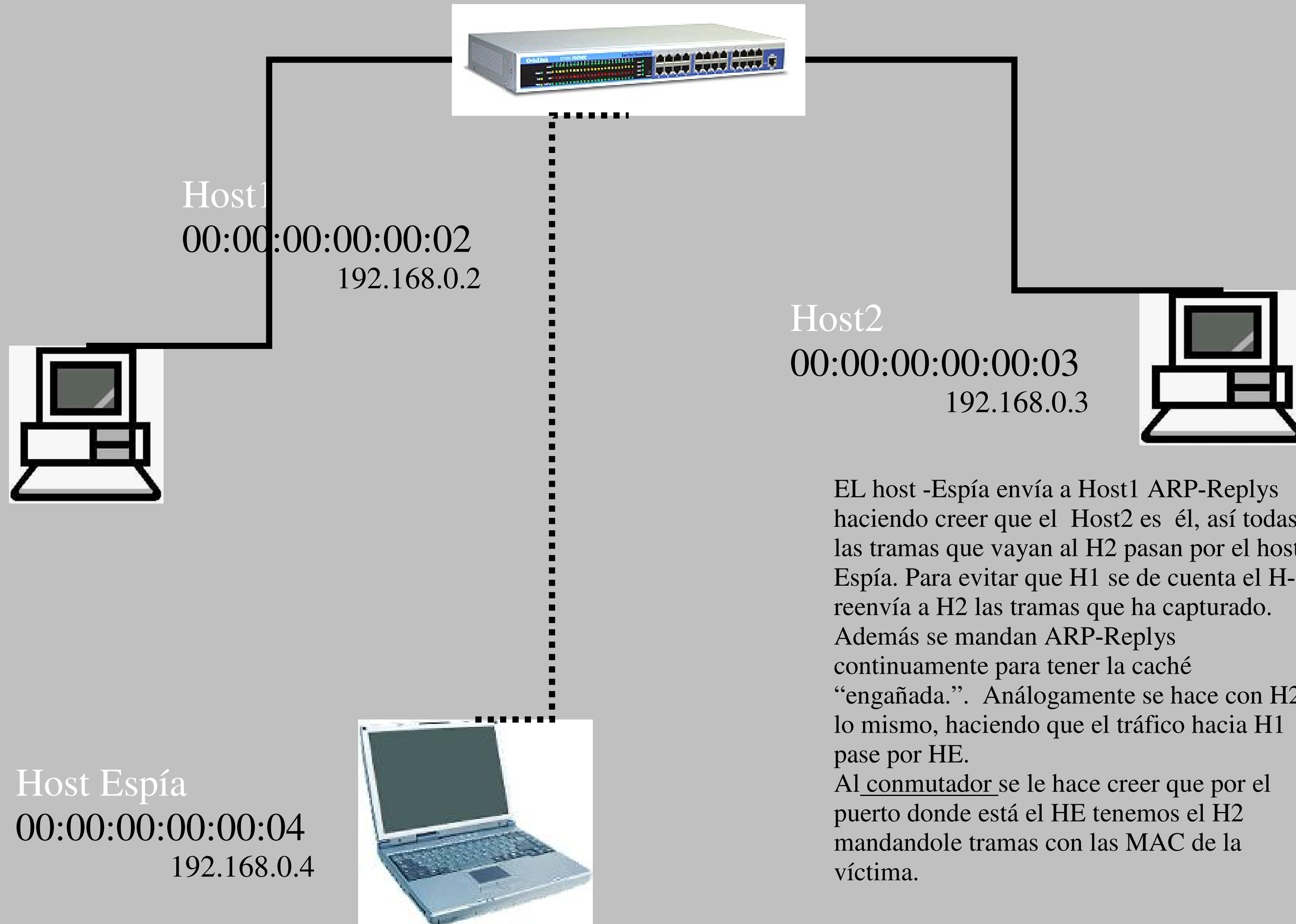
H2 Responde con un ARP-Reply con su MAC.

H1 anota en su caché que la MAC 00:00:00:00:00:02 es de la máquina con ip 192.168.0.3

El mismo procedimiento para el host2

El conmutador recibe tramas por el puerto de H1 con dirección origen MAC del host2.
El conmutador asocia al interfaz de H1 la MAC1. La trama la manda por inundación por que no conoce a que interface corresponde. Cuando H2 contesta ya sabe cual es el interface por el que lo debe de enviar porque ya lo tiene en sus tablas. Anota el par MAC-puerto para H2.

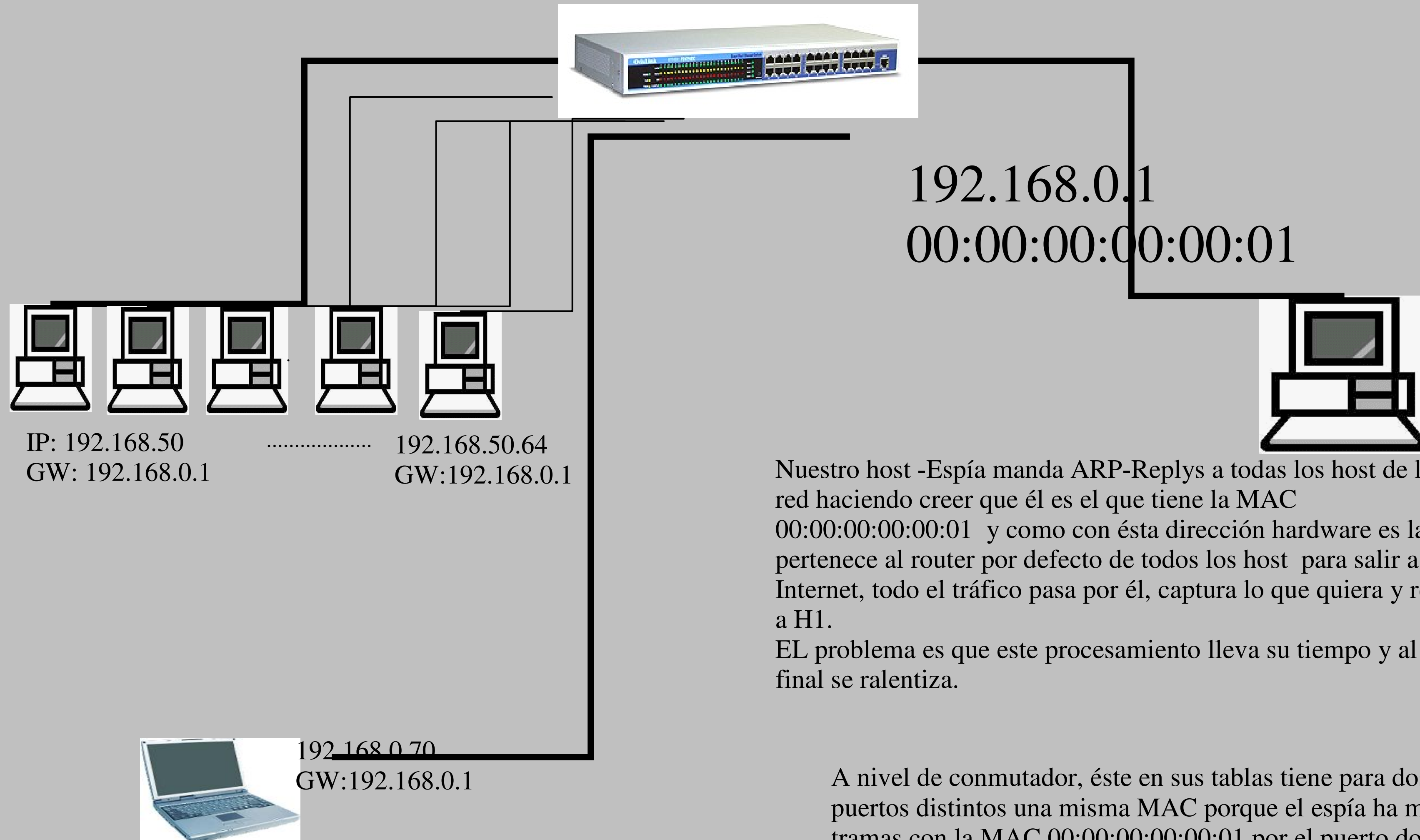
Envenenamiento ARP



EL host -Espía envía a Host1 ARP-Replys haciendo creer que el Host2 es él, así todas las tramas que vayan al H2 pasan por el host-Espía. Para evitar que H1 se de cuenta el H-E reenvía a H2 las tramas que ha capturado. Además se mandan ARP-Replys continuamente para tener la caché "engañada.". Análogamente se hace con H2 lo mismo, haciendo que el tráfico hacia H1 pase por HE.

Al conmutador se le hace creer que por el puerto donde está el HE tenemos el H2 mandandole tramas con las MAC de la víctima.

Nuestro escenario



Nuestro host -Espía manda ARP-Replys a todas los host de la red haciendo creer que él es el que tiene la MAC 00:00:00:00:00:01 y como con ésta dirección hardware es la que pertenece al router por defecto de todos los host para salir a Internet, todo el tráfico pasa por él, captura lo que quiera y reenvía a H1.

EL problema es que este procesamiento lleva su tiempo y al final se ralentiza.

A nivel de conmutador, éste en sus tablas tiene para dos puertos distintos una misma MAC porque el espía ha mandado tramas con la MAC 00:00:00:00:00:01 por el puerto donde está conectado. Y para el puerto Espía tendría en sus tablas dos MAC's, la falsificada y la propia.

Ettercap

```
Eterm
Eterm   Font   Background   Terminal

ettercap 0.6.4

1970 hosts in this LAN (81.202.33.200 : 255.255.240.0)
 1)  81.202.33.200      1)  81.202.33.200
 2)  81.202.32.1        2)  81.202.32.1
 3)  81.202.32.2        3)  81.202.32.2
 4)  81.202.32.4        4)  81.202.32.4
 5)  81.202.32.5        5)  81.202.32.5
 6)  81.202.32.6        6)  81.202.32.6
 7)  81.202.32.9        7)  81.202.32.9
 8)  81.202.32.10       8)  81.202.32.10
 9)  81.202.32.12       9)  81.202.32.12
10)  81.202.32.13      10)  81.202.32.13
11)  81.202.32.16      11)  81.202.32.16
12)  81.202.32.17      12)  81.202.32.17
13)  81.202.32.18      13)  81.202.32.18
14)  81.202.32.20      14)  81.202.32.20
15)  81.202.32.21      15)  81.202.32.21
16)  81.202.32.22      16)  81.202.32.22
17)  81.202.32.25      17)  81.202.32.25
18)  81.202.32.27      18)  81.202.32.27
19)  81.202.32.29      19)  81.202.32.29
20)  81.202.32.31      20)  81.202.32.31
21)  81.202.32.32      21)  81.202.32.32
22)  81.202.32.33      22)  81.202.32.33
23)  81.202.32.34      23)  81.202.32.34
24)  81.202.32.35      24)  81.202.32.35
25)  81.202.32.38      25)  81.202.32.38

Your IP: 81.202.33.200 MAC: 00:C0:DF:13:F6:C9 Iface: eth0 Link: SWITCH

Host: 81-202-32-1.user.ono.com (81.202.32.1) : 00:05:00:E6:B2:D8
```

Entrando en el servidor

También se puede inundar las tablas del conmutador con MAC's falsas de tal manera que el conmutador no encuentra la dirección destino en sus tablas y la manda por broadcasting.

El Hacker captura sesiones telnet, captura el usuario y password.

Aunque no accedíamos como root sino con usuario normal y setuidabamos (su) el hacker logró explotar una bug del kernel en una función de llamada al sistema ptrace para ver el estado de un proceso hijo. Éste bug está presente en todos los kernels anteriores a 2.4.21. http://lists.debian.org/debian-security/2003/debian-security-200304/msg00118.htm

El problema de éste ataque es que permite capturar sesiones encriptadas SSH1, SSL, creando certificados falsos. Por ejemplo, H1 y H2 y E(espía) capturamos el establecimiento de conexiones de A, a continuación enviamos a B un certificado idéntico al de A pero con ip la de la maquina E, al mismo tiempo enviamos un certificado falso a A así todo el tráfico pasa sin encriptar por E.

¿Cómo evitarlo?

La solución óptima es configurar los puerto del conmutador como seguros.

Se puede asociar a un puerto una o varias MACs para que filtre todas las tramas que no lleven en su dirección origen alguna de esas MACs.

En los switch cisco por ejemplo esto sería algo como:

Console> (enable) set port security 2/1 enable

Console> (enable) set port security 2/1 enable 00-90-2b-03-34-0

No todos los conmutadores permiten esto. Cisco si. ***http://mailman.argo.es/pipermail/hacking/2001-September/000677.html***

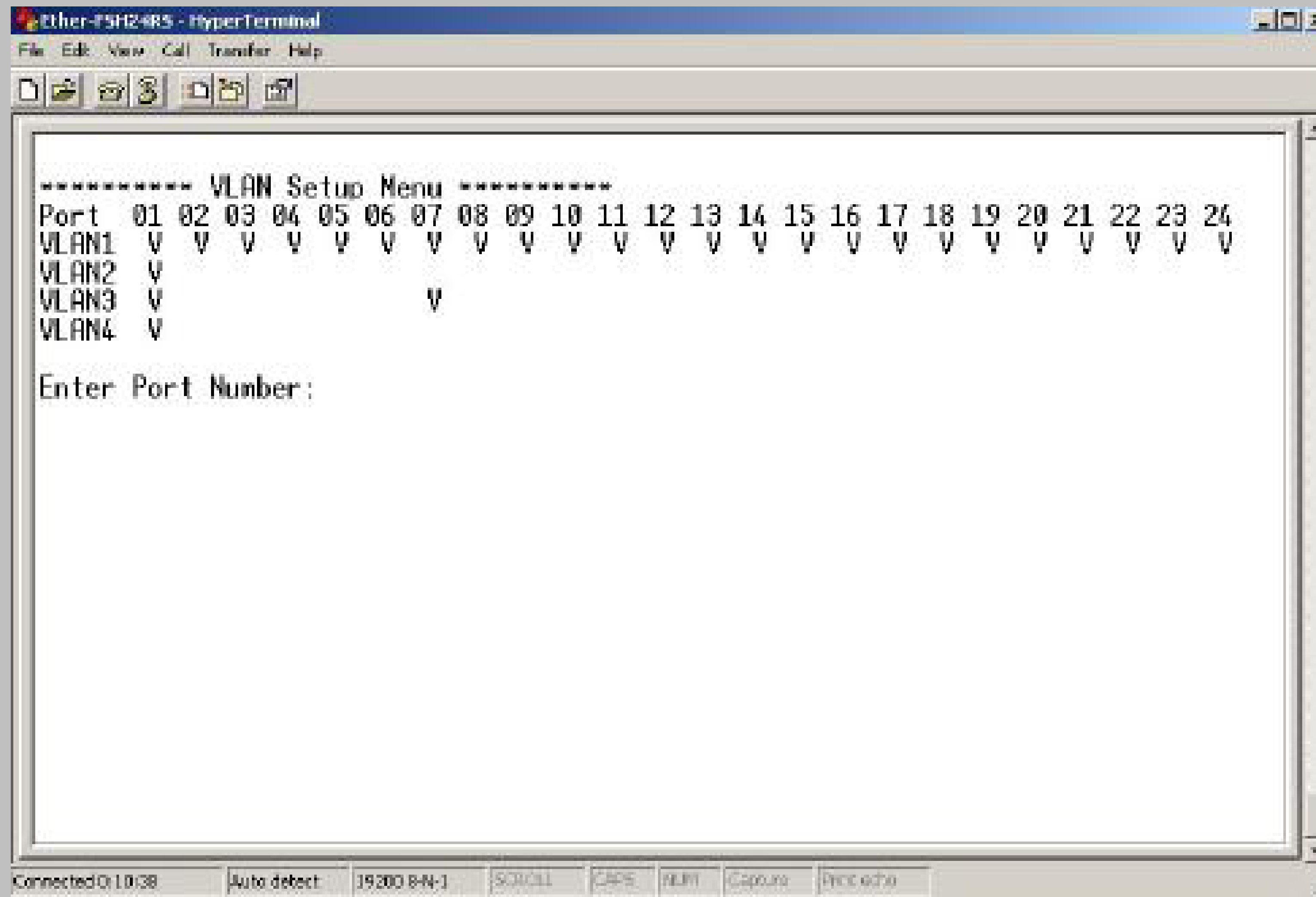
Nuestro conmutador no permite ésta configuración. Hay que idear algo.

Crearemos VLANS en el conmutador aislando el tráfico de las conexiones de portátiles

Añadimos una tarjeta de red al servidor y tenemos dos redes independientes

Hacemos NAT para las dos redes pero entre ellas no se ven.

Creando VLANS



Situación final

Eth0 conectada al router ADSL 3com

Eth1 conectada a VLAN1 192.168.0.1

Eth2 conectada a VLAN2 192.168.1.1

VLAN1: conectamos todos los ordenadores de la biblioteca y la casa de cultura

VLAN2: latiguillos de los portátiles y el cable hacia eth2

Usamos la aplicación shorewall para hacer NAT y filtrar el tráfico. Iptables también permite filtrar por MAC.

Algo así haríamos si lo hiciéramos a algo

```
echo 1 > /proc/sys/net/ipv4/ip_forward
iptables --flush
iptables --table nat --flush
iptables --table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE
iptables --append FORWARD --in-interface eth1 -j  ACCEPT
Iptables --append FORWARD --in-interface eth2 -j  ACCEPT
```

Tenemos dos redes 192.168.0.0 y 192.168.1.0

Actualizaciones servidor

Nueva versión del núcleo 2.4.21 libre de bugs.

Cambiamos el acceso vía shell por ssh2 en vez de telnet. Encriptamos.

Se desactivaron el acceso a shell a las cuentas que no se usan como tal, como la que accede para hacer las búsquedas en la base de datos OPAC1. (/bin/false)

Otros ataques

MAC Flooding: Inundar el conmutador para que mande las tramas por broadcasting.

MAC duplicating: ponerse la MAC de otra tarjeta así el tráfico también es enviado por ese interface.

Ifconfig eth0 down

Ifconfig eth0 hw ether 000000000005

Ifconfig eth0 up

Ataques de Spanning-Tree: Se envía desde un host BPDU's con el objetivo de recalcular el árbol libre de bucles. Consecuencia: Denial Of Service, mientras se recalcula el árbol no se retrasmiten tramas. También se puede enviar BPDUs con prioridad máxima para que el usuario atacante quede como raíz y vea tráfico que no debería ver, para ello el atacante debe estar conectado a dos conmutadores a la vez. Todo esto es posible si se tiene software adecuado por ejemplo para generar BPDUs. ***http://usuarios.lycos.es/elvenbyte/index.php?pagina=stp***

Programas alternativos

ARP-FUN, ARP-TOOL, DNIFF.

DNIFF: soporta más de 30 protocolos, algunos de ellos estándar y otros propietarios.

-FTP, Telnet, SMTP, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin,RIP, OSPF, PPTP MS-CHAP, NFS, YP/NIS, SOCKS, X11, CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker, Citrix ICA, Symantec pcAnywhere, NAI Sniffer, Microsoft SMB, Oracle SQL*Net, Sybase et Microsoft SQL

Permite capturar sesiones SSL y presentarse certificados ilegítimos

Otros usos de envenenamiento ARP

ARP-Spoffing es usado para sistemas de backup y de tolerancia a fallos. Mediante IP alias y ARP-Spoofing permitimos que un servidor adopte la identidad del servidor que se ha caído.

Detección de ARP-Spoffing

Evitar el ARP-Spoffing sin los conmutadores adecuados es muy difícil.

Hay programas que permiten avisar al administrador de una red de ataques ARP.

ARPwatch monitoriza los pares MAC/IP y alerta cuando hay un cambio.

Se debe de monitorizar el tráfico y comparándolo con una base de datos

Otros programas toman secuencias IP/MAC y periódicamente preguntan las actualizaciones en la red.

Estos métodos resultan farragosos cuando por ejemplo se dispone de un servidor DHCP que asigna las IP's dinámicamente

Otra solución, aparte de comprar un conmutador “100% against sniffing” es hacer que los datos vayan encriptados aunque esta medida sobrecargue el procesamiento de los datos y añada complejidad en las configuraciones.

Conclusiones

Para usar este tipo de ataques no se necesita conocimientos específicos de programación. Al alcance cualquiera.

Existen muchos programas para éste tipo de ataques.

En situaciones con muchos usuarios, como redes académicas, controlar éste tipo de ataques porque permiten ver todo el tráfico de un segmento de red pudiendo permitir averiguar información de usuarios, contraseñas, etc.

No está demás controlar el las tablas MAC/IP para ver si existe algún tipo de duplicidad o cambio que puedan inducir a un ataque.

Siempre se pueden automatizar logs, scripts, etc., para que manden periódicamente información al administrador.

En última instancia se puede aislar las tramas de una MAC mediante iptables.

Es importante conocer las características del conmutador antes de comprarlo y ver si está preparado para éste tipo de ataques.